W

NetStalker and HP OpenView

NetStalker and HP Openview invalidate the indicated claims under 35 U.S.C. § 102(b) and 35 U.S.C. § 103[*]

All text citations are taken from:

NetStalker, Installation and User's Guide, Version 1.0.2 1996 [SYM_P_0079550- SYM_P_0079629].

HP OpenView for Windows User Guide for Transcend Management Software, Version 6.1 for Windows and '97 for Windows NT, 3Com, October 1997 (hereinafter "HP OpenView for Windows User Guide") [SYM_P_0080944- SYM_P_0081098].

RFC 1157, A Simple Network Management Protocol (SNMP), May 1990 [SYM_P_0501113- SYM_P_0501142] and [SYM_P_0527111]

RFC 1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990 [SYM_P_0501012- SYM_P_0501031].

RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, March 1991 [SYM_P_0501143- SYM_P_0501205].

RFC 1271, Remote Network Monitoring Management Information Base, November 1991 [SYM_P_0501206- SYM_P_0501271].

RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2 , January 1997 [SYM_P_0603708- SYM_P_0603837]

Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 [SYM_P_0072419- SYM_P_0072641].

The text included herein are merely representative samples of the functionality of the product. I reserve the right to supplement these disclosures.

<u>102(b)</u>

NetStalker and HP OpenView were both on-sale prior to November 9, 1997. They worked together through the use of SNMP traps. Therefore, the use of the two together act as § 102(b) art. The manuals describe their operation.

[*] 103 references are identified under the heading "**<u>103:</u>**".

NetStalker and HP OpenView

Moreover, HP OpenView for Windows User Guide and RFCs 1155, 1157, 1213 and 1271 constitute a single disclosure for purposes of 35 USC § 102(b) because HP OpenView for Windows User Guide incorporates-by-reference the text of these RFCs. HP OpenView for Windows User Guide devotes several chapters to use of SNMP: *see, e.g.*, Chap. 5 "Managing SNMP Network Devices," and Chap. 7 "Custom Controls." HP OpenView for Windows User Guide specifically references and relies upon the information in these RFCs:

> "The SNMP Version 1 network devices store information about themselves in a Management Information Base (MIB).... The SNMP Manager supports all Internet MIB-II variables and can be extended to support other MIBs." (5-1) [SYM_P_0081033].
>
> "MIB-2 dependent MIBs, such as rmon, would be added t the structure under the MIB-2 group." (5-19) [SYM_P_0081051].
>
> "OpenView provides the MIBs for both MIB-2 (RFC1213) and rmon (RFC1271)." (5-20) [SYM_P_0081052].

<u>103</u>

In the alternative, NetStalker in combination with HP OpenView and RFCs 1155, 1157, 1213 and 1271 renders the patents invalid due to obviousness under 35 USC § 103. The referenced use of SNMP traps and the referenced citations provide motivation to combine the systems in order to make and improve the network traffic monitoring claimed in the patents-in-suit.

Similar disclosures and additional information are contained in the following additional references:

- HP OpenView for Windows Workgroup Node Manager User Guide, Transcend Management Software version 6.0 for Windows, 3Com, January 1997 [SYM_P_0081099-SYM_P_0081212].
- M. Siegl, and G. Trausmuth, "Hierarchical Network Management – A Concept and its Prototype in SNMPv2," 1996 [SYM_P_0500982- SYM_P_0500991].
- HP SNMP/XL User's Guide, HP 3000 MPE/iX Computer Systems Edition 5, Hewlett Packard, April 1994 [SYM_P_0076931- SYM_P_0077019].
- RFC 1441, Introduction to version 2 of the Internet-standard Network Management Framework, April 1993 [SYM_P_0501272- SYM_P_0501284].
- RFC 1757, Remote Network Management Information Base, February 1995 [SYM_P_0501319- SYM_P_0501399].

NetStalker and HP OpenView

- RFC 1451, Manager-to-Manager Management Information Base, April 1993 [SYM_P_0501285- SYM_P_0501318].
- Mark Miller, Managing Internetworks with SNMP, Second Edition, 1997 [SYM_P_0503966- SYM_P_0504693].
- Archived pages from the Haystack website, produced as [SYM_P_0504942- SYM_P_0504946].
- R. Power & R. Farrow, "Detecting Network Intruders," Network Magazine, October 1997, pp. 137-138 [SYM_P_0078627- SYM_P_0078630].

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	"What is *NetStalker* and what does it do for you? *NetStalker* provides real time monitoring and analysis of network events. . . . *NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real time using information stored in an internal database, the misuse signature database. Depending on how you configure *NetStalker*, it can also generate detailed reports from the recorded data." p. 1-2. [SYM_P_0079560] "For each alarm generated by *NetStalker*, you can configure one or more alarm handlers to serve as communications channels from *NetStalker* to you, to other network management tools or to respond to the alarm." p. 4-2. [SYM_P_0079584] "Simple Network Management Protocol - calls a shell to send an SNMP trap. The results of that trap is dependent on your site." p. 6-15. [SYM_P_0079607] *See also* Table 4-1 (SNMP Alarm Handler; Syslog Alarm Handler). P. 4-4. [SYM_P_0079586]	"The HP OpenView Workgroup Node Manager is a "platform" for network management programs. It provides a standard graphic interface so that multiple network applications can share a common display and alarm system. In addition, it provides basic network management functions to interface with devices on the network." (1-1) [SYM_P_0080957] "Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p 4) [SYM_P_0527111]
	deploying a plurality	"Before *NetStalker* can protect your network, you must	"Devices in the network are displayed on maps. Devices and subnetworks

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
	of network monitors in the enterprise network;	configure the program for your site by setting up the routers to be monitored." p. 3-1. [SYM_P_0079577] "*NetStalker* has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and *NetStalker*." p. 1-4. [SYM_P_0079562] "You add to the client list all the routers that this copy of *NetStalker* can monitor. To add a router, do the following: 1. Deselect any client router names highlighted in the *NetStalker* window. 2. From the menu bar, select **Configure**; then select **Client Information** to display the Create New Client window. Use this window to enter all the client router information." p. 3-2. [SYM_P_0079578] "What is *NetStalker* and what does it do for you? *NetStalker* provides real time monitoring and analysis of network events. . . . *NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol	can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background." (1-2) [SYM_P_0080958] "**Trapping** Some devices can send messages when certain conditions occur. The conditions may be startup, shutdown, data error, or a preset level of activity. The message resulting from a device condition is called a trap. ... Once devices are configured to send traps to the OpenView console, they will be recorded in the alarm log by default. You can customize how OpenView responds to traps using the Customize Traps dialog. You can select which traps to respond to. The traps can be of particular types or from particular device classes. ... When OpenView receives a trap message OpenView converts it into an alarm and processes it through the alarm system." (1-5) [SYM_P_0080961] "Other symbols in the Compound Object category are used for devices that provide internal configuration information to OpenView. If a supporting application is installed, opening one of these could display hardware configuration and status, memory usage, disc space, or installed software.... The **Component** symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
		vulnerabilities in real time using information stored in an internal database, the misuse signature database. Depending on how you configure *NetStalker,* it can also generate detailed reports from the recorded data." p. 1-2. [SYM_P_0079560] "For each alarm generated by *NetStalker,* you can configure one or more alarm handlers to serve as communications channels from *NetStalker* to you, to other network management tools or to respond to the alarm." p. 4-2. [SYM_P_0079584] "Simple Network Management Protocol - calls a shell to send an SNMP trap. The results of that trap is dependent on your site." p. 6-15. [SYM_P_0079607] *See also* Table 4-1 (SNMP Alarm Handler; Syslog Alarm Handler). P. 4-4. [SYM_P_0079586]	delete symbols from the standard set." (3-14) [SYM_P_0080996] "One of the keys to using the SNMP Manager is understanding the structure of the MIBs. … MIB-2 dependent MIBs, such as **rmon**, would be added to the structure under the MIB-2 group." (5-19) [SYM_P_0081051] ---------------------------------- "Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices … An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208] "Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p 4) [SYM_P_0527111] "The SNMP models all management agent functions as alterations or inspections of variables. Thus, a protocol entity on a logically remote host

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
			(possibly the network element itself) interacts with the management agent resident on the network element in order to retrieve (get) or alter (set) variables. … The strategy implicit in the SNMP is that the monitoring of network state at any significant level of detail is accomplished primarily by polling for appropriate information on the part of the monitoring center(s). A limited number of unsolicited messages (traps) guide the timing and focus of the polling." (RFC 1157 p. 6) [SYM_P_0501115]
	detecting, by the network monitors, suspicious network activity	"Table 3 is a list of the actions that may take place when a datagram satisfies a pattern. Table 3. PCF Actions **Action** **Parameters** alarm *severitynumber* clone_to *ipaddr* copy_to *ipaddr [portnum]*" Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 at Appendix C page 197 "*NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal	**"Configuring Alarms** Applications monitor the state of network devices and processes and can trigger alarms. The alarms alert network managers of changes in the status of a device or group of devices. When an application detects a change in a device status, it can request OpenView to do one or more of the following: … Forward an alarm to another management console Sound an alarm" (4-21) [SYM_P_0081019] "Critical alarms are grouped before warning alarms, and alarms within status groups are displayed in chronological order." (4-23) [SYM_P_0081021] "The OpenView SNMP custom controls provide visual indications of the values of SNMP variables for any SNMP device. .. The controls also have an Alarm capability which allows you to set low and high thresholds which will cause the control to change from normal to alarm colors when those thresholds are exceeded." (7-1) [SYM_P_0081059]

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
		database, the misuse signature database." p. 1-2. [SYM_P_0079560] "Misuse Detector combines a series of filters to "sieve" the router event data with a very efficient pattern matching signature analysis engine. Each filter reduces the total number of events sent to the next filter. The result is a set of all events that match the specified filters. An alarm is generated if specified thresholds are met." p. 6-2. [SYM_P_0079594]	"MaxThreshold Defines the upper limit for this variable. If the variable exceeds this value, and there is not an outstanding alarm condition, an alarm event will be generated and the control will be displayed in AlarmColor if Alarm=Max/Min Thresholds. If the Trap property is set to TRUE an OpenView alarm will be sent to the AlarmManager." (7-6) [SYM_P_0081064] "MinReset Defines the value that the variable must reach, after crossing the threshold, to reset the alarm condition." (7-7) [SYM_P_0081065] "MinThreshold Defines the lower limit for the variable. If the variable drops below this value, and there is not an outstanding alarm condition, an alarm event will be generated and the control will be displayed in AlarmColor if Alarm=Max/Min Thresholds. If the Trap property is set to TRUE an OpenView Alarm will be sent to the AlarmManager." (7-7) [SYM_P_0081065] "Trap Trap is used to tell the control whether to send an SNMP Trap packet whenever alarm conditions are set or cleared… If set to True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
			alarm condition to be cleared. These traps will result in alarms in the OpenView Alarm Log." (7-8) [SYM_P_0081066] "**Trap** – tells the control whether to send an SNMP Trap packet whenever alarm conditions are set or cleared. If False (default) no SNMP Traps will be sent. If True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an alarm condition to be cleared. … One of the methods to indicate alarms is to determine a *normal operating range* for a particular variable." (7-11) [SYM_P_0081069] "Many variables do not fit into the standard threshold definition. For example, a port on an Ethernet hub might have a variable that represents 'link status' … To provide support for these variables, another form of thresholds has been provided with two additional properties. These properties are **NormalValues** and **AlarmValues**." (7-12) [SYM_P_0081070] ---" • Problem Detection and Reporting The monitor can be configured to recognize conditions, most notably error conditions, and continuously to check for them. When one of these conditions occurs, the event may be logged, and management stations may be notified in a number of ways. • Value Added Data Because a remote monitoring device represents a network resource dedicated exclusively to network management functions, and because it is

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
			located directly on the monitored portion of the network, the remote network monitoring device has the opportunity to add significant value to the data it collects. For instance, by highlighting those hosts on the network that generate the most traffic or errors, the probe can give the management station precisely the information it needs to solve a class of problems." (RFC 1271 p. 3-4) [SYM_P_0501208- SYM_P_0501209] "The Event group controls the generation and notification of events from this device. Each entry in the eventTable describes the parameters of the event that can be triggered. Each event entry is fired by an associated condition located elsewhere in the MIB. An event entry may also be associated with a function elsewhere in the MIB that will be executed when the event is generated. For example, a channel may be turned on or off by the firing of an event. Each eventEntry may optionally specify that a log entry be created on its behalf whenever the event occurs. Each entry may also specify that notification should occur by way of SNMP trap messages. In this case, the community for the trap message is given in the associated eventCommunity object. The enterprise and specific trap fields of the trap are determined by the condition that triggered the event. Three traps are defined in a companion document: risingAlarm, fallingAlarm, and packetMatch." (RFC 1271 p. 67) [SYM_P_0501267]
	based on analysis of network traffic data selected from the	"*NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies	"The Simple Network Management Protocol (SNMP) Version 1 is a standard that defines a method of communicating with and controlling network devices. Devices that support SNMP V.1 standard can be queried

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
	following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests. network connection denials, error codes included in a network packet};	network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560] "Misuse Detector combines a series of filters to "sieve" the router event data with a very efficient pattern matching signature analysis engine. Each filter reduces the total number of events sent to the next filter. The result is a set of all events that match the specified filters. An alarm is generated if specified thresholds are met." p. 6-2. [SYM_P_0079594] "There are four filters included in the Misuse Detector window. The filters are • Packet • Packet Type • Network • Event The window also contains lists of Misuse Signature Groups, Misuse Detection Signatures, and Alarm Types." p. 6-5. [SYM_P_0079597] **"Packet**	for their status and other device information. … OpenView provides an SNMP Management function that can be used to communicate with SNMP devices. The device settings and other device information are available as variables and are defined either in a standard Management Information Base (MIB) file or in a custom MIB file proved by the device manufacturer." (1-7) [SYM_P_0080963] "**DataType** – can be set to Absolute or Delta. This tells the control whether to display the actual value that was returned from the SNMP device (Absolute) or the difference in the variable since the last poll (Delta). The Text Box control could be used to poll the UDPInDatagrams of a device. If you set the DataType of the control to Absolute, you will see a constantly incrementing value displayed which is the total since the last delivery reset. If you set DataType to Delta, you will see a number that represents the number of UDPInDatagrams since the last poll." (7-10) [SYM_P_0081068] -- "ifInUnknownProtos OBJECT-TYPE … DESCRIPTION 'The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.'" (RFC 1213 p. 19) [SYM_P_0501161] "ifOutErrors OBJECT-TYPE … DESCRIPTION 'The number of outbound packets that could not be transmitted because of errors.'" (RFC 1213 p. 20) [SYM_P_0501162]

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
		The Packet filter queries the events by the protocol used to transmit the packet. When you select the Protocol filter, the Select Internal Protocols window is displayed (Figure 6-3). Select from the list of available network protocols, which includes ip, icmp, ggp, tcp, egp, pup, udp, hmp, xns-idp, and rdp. For example, when you select tcp from the list, all events using the tcp protocols including telnet and ftp are returned, but no events using any other protocol are returned." p. 6-6. [SYM_P_0079598] "**Packet Type** ***ICMP Type*** The Packet Type filter queries the events by ICMP type, TCP service, or UDP service. When you select ICMP Type, the Select ICMP Packets by Type window is displayed (Figure 6-4). Select from the Object Type list, which includes echo reply, destination unreachable, source quench, redirect, echo request, time exceeded for a datagram, parameter problem on a datagram, time stamp request, time stamp reply, and information request." p. 6-7. [SYM_P_0079599] "***TCP/UDP Service***	"ipInHdrErrors OBJECT-TYPE… DESCRIPTION 'The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.'" (RFC 1213 p. 24) [SYM_P_0501166] "icmpInErrors OBJECT-TYPE … DESCRIPTION 'The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.)'" (RFC 1213 p. 36-37) [SYM_P_0501178- SYM_P_0501179 "tcpActiveOpens OBJECT-TYPE … DESCRIPTION 'The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.'" (RFC 1213 p. 42) [SYM_P_0501184] "tcpPassiveOpens OBJECT-TYPE… DESCRIPTION 'The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.'" (RFC 1213 p. 42) [SYM_P_0501184] "tcpAttemptFails OBJECT-TYPE … DESCRIPTION 'The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.'" (RFC

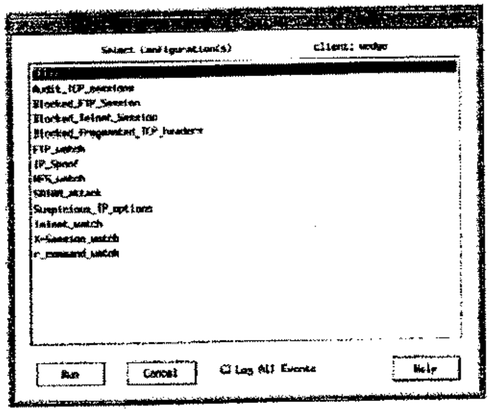
NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
		When you select TCP Service or UDP Service, the List Network Ports window is displayed (Figure 6-5). Select from the list of Internet services such as systat, ftp, telnet, www, and Gopher. By selecting appropriate services, you can closely watch specific network activity." p. 6-8. [SYM_P_0079600] "**Network** The Network filter queries events based on the origin or destination of the connection to the router using the network address for internal or external connections. Network addresses contain the individual addresses, the classes of the addresses, and sets of individuals/classes." p. 6-10. [SYM_P_0079602] "***Types*** **Events** The Events filters query the router events based on router event types or PCF filters installed at the router. The Event Types filter examines the data for specific events or classes of events. When you select Event Types, the Configure Event Types window is displayed (Figure 6-11). Ten event classes are listed, of which nine are for router events and one is for PCF filter events. For more information about router event	1213 p. 42-43) [SYM_P_05001184- SYM_P_0501185] "tcpOutRsts OBJECT-TYPE … DESCRIPTION 'The number of TCP segments sent containing the RST flag.'" (RFC 1213 p. 46) [SYM_P_0501188] "etherStatsOctets OBJECT-TYPE … DESCRIPTION 'The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octents).'" (RFC 1271 p. 13) [SYM_P_0501218] "etherStatsPkts OBJECT-TYPE … DESCRIPTION The total number of packets (including error packets) received.'" (RFC 1271 p. 13) [SYM_P_0501218] "The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured." (RFC 1271 p. 24) [SYM_P_0501229] See table in my expert report.

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
		types, see the NSC manual for your router." p. 6-12. [SYM_P_0079604] *"Filters* Use Filters to examine all events associated with the PCF filters. When you select **Filters**, the List Objects by Name window is displayed (Figure 6-12) with a list of all PCF filters. (See Chapter 2 for a description of these filters.) You can create a list of filters by using **Insert** or **Remove**. *NetStalker* searches for these names in the event stream and returns the event when a match occurs." p. 6-13. [SYM_P_0079605] "**Understanding Misuse Detector Signatures** Misuse Detector analyzes events for evidence of misuse or misuse "signatures." Misuse is defined as any activity that would be deemed unacceptable and undesirable were it known to the party responsible for the security of the machine. It uses Haystack Labs' proprietary database of misuse signatures of: • Known attacks • Attempts to exploit known system vulnerabilities • Typical outcomes of system attacks. Including known outcomes of attacks provides a "safety net" to	

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
		capture misuse that results from attacks not represented in the set of known signatures. The misuse signatures are obtained from a variety of sources including organizations that have been targets of misuse. The results are an identified misuse and a set of events that constitute the identified misuse." p. 6-14. [SYM_P_0079606]  Select Configuration(s) client: wedge Audit_TCP_sessions Blocked_FTP_Session Blocked_Telnet_Session Blocked_Fragmented_TCP_headers FTP_watch IP_Spoof NFS_watch SATAN_attack Suspicious_IP_options Telnet_watch X-Session_watch r_command_watch Run Cancel ☐ Log All Events Help **FIGURE 5-2** Run *NetStalker* window p. 5-7. (SYM_P_0079592]	

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
	generating, by the monitors, reports of said suspicious activity; and	"Table 3 is a list of the actions that may take place when a datagram satisfies a pattern. Table 3. PCF Actions **Action** **Parameters** alarm *severitynumber* clone_to *ipaddr* copy_to *ipaddr [portnum]*" Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 at Appendix C page 197. "The next step in creating a custom misuse detection configuration to select one or more alarms and to assign the parameters for triggering the alarm. In the Configure Alarm Handler window, you created the alarm configurations (See Chapter 4). In the Configure Misuse Detector window, you activate the alarms for specified Misuse Detector configurations. To activate an alarm, select the alarm type from the displayed list." p. 6-15. [SYM_P_0079607] See "Alarm Types" pp. 6-15 to 6-17. [SYM_P_0079607-	"Some devices can send messages when certain conditions occur. The conditions may be startup, shutdown, data error, or a preset level of activity. The message resulting from a device condition is called a trap. … Once devices are configured to send traps to the OpenView console, they will be recorded in the alarm log by default. You can customize how Openview responds to traps using the Customize Traps dialog. You can select which trap to respond to. … When OpenView receives a trap message OpenView converts it into an alarm and processes it through the alarm system." (1-5) [SYM_P_0080961] "**Applications and Alarms** Equipment manufacturers create application programs to provide information on the status of their devices. Application programs can request status information from the device, make device settings, or run device diagnostics. The application program then sends the appropriate information to OpenView as alarms." (1-6) [SYM_P_0080962] "**Monitoring Traps from Network Devices** Traps are specific types of messages that are generated by some devices to indicate a change in their status. When a device is installed on the network part of its installation procedure is to enter the address of a management console where these traps are to be sent. Refer to the device installation and configuration documentation and set the trap address to the network address of the OpenView console." (4-10) [SYM_P_0081008] "Trap is used to tell the control whether to send an SNMP Trap packet

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
		SYM_P_0079609] *"SNMP* Simple Network Management Protocol - calls a shell to send an SNMP trap. The results of that trap is dependent on your site." p. 6-15. [SYM_P_0079607] "**Email** Sends an email message containing the message severity, and trace (if requested) to the user via Unix mail." p. 6-15. [SYM_P_0079607] *"Report* Writes event information to a single report file in a default format with each event listed by severity. The default format is illustrated in Figure 6-14." p. 6-16. [SYM_P_0079608] *See also* Table 4-1, p. 4-4. [SYM_P_0079586]	whenever alarm conditions are set or cleared… If set to True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an alarm condition to be cleared. These traps will result in alarms in the OpenView Alarm Log." (7-8) [SYM_P_0081066] "**Trap** – tells the control whether to send an SNMP Trap packet whenever alarm conditions are set or cleared. If False (default) no SNMP Traps will be sent. If True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an alarm condition to be cleared. … One of the methods to indicate alarms is to determine a **normal operating range** for a particular variable." (7-11) [SYM_P_0081069] "The Simple Network Management Protocol (SNMP) Version 1 is a standard that defines a method of communicating with and controlling network devices. Devices that support SNMP V.1 standard can be queried for their status and other device information." (1-7). [SYM_P_0080963]
	automatically receiving and integrating the reports of suspicious	"*NetStalker* monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs' patent pending technology, *NetStalker* automatically identifies network attacks and attempts to exploit TCP/IP protocol	"Once devices are configured to send traps to the OpenView console, they will be recorded in the alarm log by default. You can customize how Openview responds to traps using the Customize Traps dialog. You can select which trap to respond to. … When OpenView receives a trap

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
	activity, by one or more hierarchical monitors.	vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560] "*SNMP* Simple Network Management Protocol - calls a shell to send an SNMP trap. The results of that trap is dependent on your site." p. 6-15 [SYM_P_0079607]	message OpenView converts it into an alarm and processes it through the alarm system." (1-5) [SYM_P_0080961] "**Alarms** Changes in device status or "alarms" provide the notification to the OpenView map that a noteworthy event has happened on the network. Alarms are the main mechanism used to communicate device status. Alarms are displayed on the network map and are listed in the Alarm Log. The alarms are also recorded in a Paradox database. The Alarm database allows to you generate reports or archive network performance. In addition to visual cues, alarms can be set to trigger sounds, programs, or even activate a remote paging device based on the type of alarm received." (1-3) [SYM_P_0080959] "**Alarm System** OpenView allows you to configure how alarms will be processed or displayed on maps, clear alarm conditions, and create reports from the alarm log. In addition, you can configure alarms of a particular level to start programs, send pages, or be forwarded to other workstations." (1-6) [SYM_P_0080962] "The submap symbol displays the most severe status color for all of the nodes or devices within it. This allows the most severe status information for any device in the network to be propagated up to the home submap. The home submap can then give you an overview of status for the entire network." (3-2) [SYM_P_0080984]

NetStalker and HP OpenView

'203 Claim number	Claim Term	NetStalker (public use/on sale)	HP OpenView (printed publication and public use)
			"OpenView provides several different ways that you can monitor the devices in your network. You can: . . . Monitor trap messages sent by network devices alerting you to changes in device status. Configure how alarms are processed, displayed, recorded, and forwarded." (4-1) [SYM_P_0080999] "**Automatically Acknowledging Alarms Generated by Traps** The Acknowledge on Matching Trap and Variable text box allows you to clear a trap when a new specified trap is received. The original trap is moved from the current alarm log to the history alarm log. A variable in the trap packed that holds the network object's name can be selected to match the subobject field in the alarm log. This is to make sure that a trap that clears an alarm is referring to a particular device." (4-16) [SYM_P_0081014] "**Managing Alarms** Alarms generated by applications, traps, or polling are managed through the map, alarm log, and alarm forwarding functions." (4-17) [SYM_P_0081015] "**Status Propagation** You can select the way device status is propagated to higher submap levels using **Customize Alarms** in the **Options** menu. Status propagation can be